United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

IMPROVING MAGTF INTELLIGENCE SUPPORT TO INFORMATION OPERATIONS IN THE FOUR BLOCK WAR

SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF MILITARY STUDIES

Major Damian L. Spooner, USMC

AY 09-10

Mentor and Oral Defense Committee Member: Dr. Bruce E. Bechtol Jr., Ph.D.

Approved:_____

Date:_____

Oral Defense Committee Member: Dr. Douglas E. Streusand, Ph.D.

Approved:_____

Date:_____

Table of Contents

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Executive Summary

Title: Improving MAGTF Intelligence Support to Information Operations in the Four Block War

Author: Major Damian L. Spooner, USMC

Thesis: The increasingly important role of information operations (IO) requires the Marine Corps to refine doctrine, training, organization and focus in order to improve overall MAGTF intelligence support to IO.

Discussion: Recent conflict demonstrates the Three Block War concept is an accurate description of the challenges facing the MAGTF in many parts of the world. Additionally, the increased importance of IO demonstrates the Four Block War concept, with the fourth block being information, requires the MAGTF intelligence organization to provide tailored and dedicated support to IO and associated disciplines. Although several doctrinal publications and handbooks exist regarding IO, few provide intelligence personnel with practical and detailed guidance on how to perform analysis and construct products specifically designed for use by IO planners and implementers. Recent examples in Iraq and Afghanistan demonstrate the need for an enhanced focus on IO and particularly for a dedicated intelligence effort. The creation of the Marine Corps Information Operations Center (MCIOC) in Quantico illustrates the Marine Corps' recognition of the importance of IO and the need to enhance overall support to the MAGTF. The MCIOC is on the forefront of developing the necessary training and tools to improve intelligence support. The MCIOC's efforts will not only improve current intelligence support, but their efforts with the Training and Education Command (TECOM) will also ensure Marine intelligence personnel are prepared to provide improved support to IO in the future.

Conclusion: The ability of MAGTF intelligence professionals to provide the required intelligence support to IO can be enhanced through improvements to doctrine, an IO emphasis in training, the establishment of specific IO population-centric intelligence cells at the tactical level, the development and maintenance of IO specific base-line intelligence products and the development of collaborative communities to counter enemy IO efforts. The following recommendations provide actions that can improve overall intelligence support to IO.

- Develop tactics, techniques and procedures for intelligence analysts conducting IPB in support of IO.
- Encourage MAGTF intelligence personnel to have a proactive IO focus and ensure they have the tools and training to support IO and Public Affairs (PA) efforts.
- Ensure IO billets are filled to 100 percent at all MAGTF levels.
- Ensure IO trained intelligence analysts are pushed down to the battalion and company levels.
- Create "information centers" separated from intelligence centers where population centric information can be gathered and exchanged.
- Ensure all MAGTF intelligence personnel understand the roles and capabilities of the MCIOC and how to leverage those capabilities.
- Incorporate tailored IO training in all MAGTF intelligence instruction at NMITC.
- Establish the requirement for and provide support to the development of an IO JESP.
- Spearhead the development of virtual IO collaborative communities to assist in monitoring and countering adversary IO.

PREFACE

The importance of information operations (IO) is clear to those personnel who operated in Iraq and Afghanistan and watched insurgents utilize local media and word of mouth to manipulate the local population against coalition forces. In recent conflicts, we watched the insurgents capitalize on our lack of IO preparedness and take advantage of our misunderstanding of the local culture and situation. As an intelligence officer, I was often frustrated with the inability of our intelligence structure as a whole to identify aspects of the local area not specifically enemy related. Although we could spend hours or days identifying and tracking the latest "bad guy" to enter the area, we were generally unable to identify the key leaders and specific requirements of the community that would enable us to begin winning over the population. Additionally, the limited attention paid to information operations ensured the insurgents maintained the upper hand. Although we would distribute posters and attempt to get the word out about operations and humanitarian efforts, the insurgents were ready to preempt or counter our messages. In order to act proactively in information operations, it is essential for intelligence personnel to have the tools, training and organization necessary for success.

The Marine Corps has taken some incredible steps to improve the MAGTF's IO capability. In particular, the establishment of the Marine Corps Information Operations Center (MCIOC) is central to ensuring future success. As the MCIOC develops and becomes the IO hub for the Marine Corps, MAGTF intelligence personnel will increasingly leverage their capabilities to support IO. The establishment of this center of expertise will undoubtedly improve MAGTF intelligence support to IO and provide intelligence personnel with much needed guidance and support.

The goal of this paper is to identify some areas where the Marine Corps can make changes to enhance the ability of MAGTF intelligence personnel to provide dedicated, tailored, accurate and timely support to IO. Although the MCIOC is certainly addressing many of the identified issues, some remain institutional and can only be accomplished by local leadership making the appropriate changes and identifying additional requirements. A further objective of this paper is to spark thought and conversation about the need for improved intelligence support to IO and the road ahead. With these goals in mind, it is my expectation that others will identify additional recommendations or improve upon those offered in this paper.

INTRODUCTION

Recent conflicts illustrate the importance of information operations (IO) in modern warfare. From the use of Twitter by Iranian dissidents to Al Qaeda's media campaigns, using information and technology to influence local and international populations is an increasingly available and effective means of shaping the environment. Although the ongoing conflicts in Iraq and Afghanistan clearly demonstrate the need for information operations, specifically as part of counter-insurgency campaigns, information operations are essential for nearly all Marine Air Ground Task Force (MAGTF) future missions. The National Intelligence Council (NIC) and other intelligence organizations predict that future conflict will occur increasingly in urban areas and involve belligerents with increasingly advanced weapons and communications technology placing additional importance on IO.[1] The Marine Corps concept of the "Three Block War," espoused by General Krulak,[2] is now a reality and information superiority is playing a progressively more important role. Marines facing the entire spectrum of tactical challenges in a span of just hours and within the space of only a few city blocks are now confronted with the additional challenge of the battle for information superiority. General Mattis' "Four Block War" concept combines General Krulak's urban battle with the necessity of defeating the enemy through the incorporation of information operations.[3] The ever-increasing importance of information operations levies additional requirements on the MAGTF intelligence structure and demands organizational and doctrinal refinement, reprioritization of training and focus as well as the development of products, tactics, techniques and procedures to improve overall intelligence support to IO.

The NIC's unclassified assessment of the world situation in 2025, entitled, "Global Trends 2025: A Transformed World," provides an important guideline for determining the likely

aspects of future conflict and possible roles of the MAGTF. The study also brings to light several key findings important when considering the role of information operations in future warfare. The report finds that although the United States will remain a superpower in 2025, the world will become multi-polar, with the U.S. sharing power with rising state and non-state actors.[4] In particular, China, India and potentially Russia will have significantly more influence in world affairs and increased military capability. Additionally, the world population is expected to increase by over 1 billion people by 2025 with 57 percent of the world's population living in urban areas compared to 50 percent today.[5] The increase in population will put a significant strain on critical resources such as fuel, water and food and likely lead to additional regional conflicts.[6] These factors indicate that the MAGTF will likely operate in more congested urban areas and contend with competing state and non-state actors, all of whom will have increased access to weapons and communications technology and media outlets. The inability of the U.S. to act unilaterally will result in the formation of temporary alliances with various state and non-state actors and put a premium on information operations from the tactical to strategic level. The need to maintain alliances and counter direct and indirect actions from adversaries and competitors requires future MAGTF operations of all scales to incorporate information operations to influence opinion, defeat the enemy, and deny the enemy access to critical friendly information.

DOCTRINE REGARDING INTELLIGENCE SUPPORT TO IO

Several pertinent doctrinal military publications and orders provide definitions and general guidance concerning the role of intelligence in support of information operations. Among these publications are Joint Publication (JP) 3-13 Information Operations, Field Manual (FM) 3-13 Information Operations: Doctrine, Tactics, Techniques, and Procedures, Marine

Corps Warfighting Publication (MCWP) 3-40.4 MAGTF Information Operations, JP 2-0 Joint Intelligence, JP 2-01.3 Joint Intelligence Preparation of the Operational Environment (JIPOE), FM 34-130 Intelligence Preparation of the Battlefield (IPB), FM 3-06 Urban Operations (Appendix B), FM 2-91.4, Intelligence Support to Operations in the Urban Environment, FM 3-24 Counterinsurgency, MCWP 2-1 Intelligence Operations, and MCO 3120.10, Marine Corps Information Operations Program. These publications and orders explain that Marine Corps Information Operations support maneuver warfare through actions that employ information to deny, degrade, disrupt, destroy or influence an adversary commander's methods, means or ability to command and control forces and to inform target audiences through informational activities.[7] Additionally, Marine Corps IO is multi-disciplined, primarily focused at the operational and tactical levels of war and conducted to enhance mission accomplishment in times of peace or war.[8] Marine Corps doctrine also explains that capabilities relevant to IO include, but are not limited to, psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), electronic warfare (EW), physical attack, information assurance (IA), computer network operations (CNO), public affairs (PA), and civil-military operations (CMO).[9]

These different aspects of IO are all supported by MAGTF intelligence to varying degrees. Importantly, Marine Corps doctrine also recommends the establishment of an appropriately staffed IO cell within the MAGTF, to include dedicated intelligence support, to participate fully in the planning process and facilitate coordination between various staff elements and organizations contributing to IO planning and execution.[10] This recommendation is not regularly adopted throughout the Marine Corps as IO billets, particularly at the lower levels, are often gapped or filled with untrained personnel or those with only a rudimentary understanding of IO.[11] Additionally, the wide breadth of knowledge required for planning and

executing effective comprehensive IO demands dedicated and relevant input with an emphasis on intelligence support.

Although the aforementioned publications provide general guidance regarding the significant intelligence requirements to support IO, there is a dearth of information regarding specific analysis, production and collection methods and techniques. The most useful doctrinal publications providing specific details regarding intelligence support to IO are JP 3-13 IO, JP 2-01.3 JIPOE, and FM 3-24 Counterinsurgency. In particular, JP-2-01.3 provides a practical example of a combined information overlay and an information system vulnerability assessment matrix that could be produced in support of IO (See Appendix A).[12] Additionally, FM 3-24 provides a useful overview of the intelligence focus and requirements for the various phases of IPB in a counterinsurgency, most of which apply to IO planning and execution during a counterinsurgency as well as other types of conflicts. These three publications also provide intelligence analysts with specific requirements, but fall short in detailing techniques for analysis and production. Another useful asset is the IO Generic Intelligence Requirements Handbook (IO-GIRH) produced by the Marine Corps Intelligence Activity (MCIA). This publication provides analysts with suggested areas of analytic concentration for various aspects of IO, but does not provide adequate guidance or detail on specific intelligence products required for IO. With the increased importance of IO, the addition of doctrinal analytical techniques and specific products based on successful operations to the current IPB process would improve intelligence analysts' ability to support IO. As indicated by Marine Officers attempting to plan and implement IO in Iraq, revising FM 34-130 or creating an additional FM to address specific intelligence support to IO would enhance the effectiveness of IO during MAGTF Operations.[13]

RECENT IO CHALLENGES AND SUCCESSES

Recent MAGTF operations demonstrate the importance of appropriate intelligence support to IO and the need to provide Marines with adequate training, equipment, and appreciation for IO. The following two examples from Fallujah respectively illustrate how the lack of IO preparation can lead to significantly negative consequences and how intelligence driven IO can significantly contribute to the overall success of an operation. During the April 2004 Fallujah campaign code-named Operation Vigilant Resolve, Marine actions at the Abdul-Aziz al-Samarai mosque resulted in negative press that contributed significantly to the premature cessation of the campaign.[14] During fighting around the mosque, snipers firing from the minaret pinned down a company of Marines unable to return effective fire due to restrictions against damaging the mosque. Following approval from legal authorities, the Marines attempted to engage the target with a Hellfire missile, but the missile missed the target and landed harmlessly in an empty field. Unwilling to risk another errant missile shot, the Marines on the ground asked to drop two bombs along the retaining wall around the mosque so they could rush the insurgents without being subjected to sniper fire while attempting to breach the wall. Following another debate and legal decision, a fixed-wing aircraft dropped two 500-pound bombs, opening a gap in the wall and allowing the Marines to enter the compound. The Marines conducted a thorough search of the mosque and discovered the insurgents had fled, leaving behind only empty shell casings. The Marines found no bodies and the only significant damage to the compound was the damage inflicted by the bombs on the retaining wall. The Marines were well aware that this event could receive negative media attention and quickly discovered that an Associated Press reporter released a supposed eyewitness account of the event.[15]

Associated Press (3:01 PM UK Time) – A U.S. helicopter fired three missiles at a mosque compound in the city of Fallujah on Wednesday, killing about forty people as American

forces battled Sunni insurgents, witnesses said. Cars ferried bodies from the scene, though there was no immediate confirmation of casualties. The strike came as worshippers gathered for afternoon prayers, witnesses said. They said the dead were taken to private homes in the area where temporary hospitals had been set up.[16]

The Marines scrambled to pull together all the facts, including unclassified video and still images in order to draft and release an accurate and convincing rebuttal to the erroneous report. Unfortunately, because the images were taken using a classified video system, it took the Marines more than eight hours to get the accurate image cropped and prepared for release. In a 24-7 news cycle, eight hours was an eternity that allowed the story to grow in distribution and inaccuracies. The story concerning the "mosque massacre" was eventually featured on BBC, Al Jazeera and several internet news websites. The full impact of this negative press reporting cannot be determined, but it is clear that it contributed to the shift in public opinion and support that resulted in the political decision to cease the assault on Fallujah.[17]

The previous situation demonstrates the necessity of adequate intelligence support to IO and the need for a better appreciation of IO. In this case, IPB products developed to determine likely key IO areas of interest such as mosques, schools, hospitals and government buildings would assist in alerting the commander of potential IO opportunities for enemy and friendly forces alike. With a focus on IO, intelligence should also determine important leadership in the area and understand their allegiances and relationship with the enemy. Most importantly, the intelligence section should have an IO mindset, conduct a detailed analysis of enemy vulnerabilities as well as friendly vulnerabilities and continually determine methods in which IO may be used to friendly or enemy advantage. In this scenario the Marines could have prepared and postured to take advantage of the fact that insurgent snipers were using a mosque as a firing position. A proactive IO intelligence posture would ensure designated Marines carried video and still digital cameras in order to document and quickly disseminate information pertinent to IO.

An intelligence section focused on IO would also be prepared to quickly assist in crafting a press release with relevant images showing snipers firing from the minaret and no damage to the mosque while also explaining that the assault on the mosque occurred on a Wednesday outside of prayer time. By being trained, equipped and focused on IO, the Marines could be the first to get the message out and not be forced to react to negative press.

Following the information challenges of Operation Vigilant Resolve, senior leaders planned for a second assault on Fallujah and fully incorporated IO and PA. Intelligence personnel worked closely with IO planners and others to fully leverage intelligence resources to develop critical IO targets for the upcoming operation. Operation Al Fajr, the second assault on Fallujah, provides an excellent example of intelligence supporting and driving the IO effort. In the areas of OPSEC and MILDEC, intelligence identified precision targets in southern Fallujah to focus the enemy's attention away from force build-up in the north. Intelligence supported psychological operations in assisting IO officers' draft messages encouraging insurgents to surrender and noncombatants to depart the city.[18] This effort was particularly successful and in some estimates resulted in approximately 90 percent of noncombatants departing.[19] Electronic Warfare was also conducted during the operation and was successful in restricting the enemy's access to certain communications and directing towards communications more easily monitored by coalition forces.

Additionally, intelligence analysis revealed that the Fallujah Hospital was one of the most significant propaganda centers used by the insurgents. This analysis enabled planners and commanders to employ the Iraqi commandos during the early stages of the battle in order to secure this critical IO terrain and significantly disrupt the enemy's ability to disseminate information.[20] Based on lessons learned from Operation Vigilant Resolve, public affairs

personnel worked closely with planners to arm troops with photographic equipment in order to document insurgent activity. These images and videos were then used to create detailed imagery and geospatial products depicting the locations and types of atrocities committed by the insurgents. Additionally, the PA personnel established rapid means for dissemination of images and video from forward units to the rear and also created an unclassified webpage where this information was quickly transferred and shared with media. This enabled media outlets to rapidly download the products and turned the information battle in favor of the coalition forces.[21]

LESSONS FROM AFGHANISTAN AND IRAQ

Although the previous examples demonstrate an improvement in intelligence support to IO, specifically in Fallujah, Iraq, the recently released assessment on intelligence in Afghanistan by Major General Michael Flynn, USA clearly illustrates that even after several years on the ground where IO should be a priority, intelligence organizations fail to focus on areas particularly important to IO. MG Flynn, the senior intelligence officer in Afghanistan, makes several important observations and recommendations concerning intelligence support to a counterinsurgency and IO. Although the focus of the paper is primarily on intelligence support to a counterinsurgency, many of the findings may be applied to intelligence support to IO in a future "Four Block War" conflict as well. The premise of MG Flynn's paper is that most intelligence organizations are focusing nearly exclusively on the enemy and neglecting to focus on determining how to positively influence the people of Afghanistan.[22] As a result, the report finds, there is a lack of useful intelligence collected, analyzed and disseminated regarding

> "…items such as: census data and patrol debriefs; minutes from shuras with local leaders; after-action reports from civil affairs officers and Provincial Reconstruction Teams (PRTs); polling data and atmospherics reports from psychological operations and female engagement teams; and translated summaries of radio broadcasts that influence local farmers, not to mention the field observations of Afghan soldiers, United Nations officials, and non-governmental organizations (NGOs)."[23]

The report illustrates the tendency of intelligence personnel to overemphasize information about the enemy at the cost of the political, economic and cultural environment.[24] The paper also finds that due to the concentration on the enemy and lack of collection and analysis on population-centric information, brigade and regional intelligence products provide units with little they did not already know.[25] Additionally, the report makes clear that the doctrinal battalion S2 organizational construct does not contain enough analysts to effectively conduct intelligence.[26] MG Flynn identifies the roots of the problem as attitudinal, cultural, and human with the intelligence community passive about aggregating information that is not directly enemy related.[27] Based on these findings, the report offers several excellent recommendations for the current conflict that are also applicable to improving intelligence support to IO in the future "Four Block War."

The recommendations offered in the report that are the most pertinent to improving MAGTF intelligence support to the "Four Block War" focus on improving the organization of intelligence personnel throughout the chain of command and the focus of intelligence collection, analysis and dissemination. Based on interaction with successful units on the ground, MG Flynn recommends distributing intelligence personnel from higher echelons down to the company level in order to address the demanding requirements at the tactical level and provide intelligence personnel at higher levels with an improved understanding of what is occurring at the grass roots level.[28] These Company-Level Intelligence Cells (CLICs), often augmented with organic infantry personnel, create a network of human sensors able to debrief patrols, observe key personalities and terrain across an area, and most importantly record and disseminate their findings. Additionally, successful intelligence organizations ensure the flow of information

through digital and voice communications and include critical information such as patrol debriefs, notes of officers who meet with local leaders, the observations of civil affairs officers, and HUMINT reports. This information is then consolidated, analyzed and disseminated, resulting in an improved focus and understanding as well as updated intelligence requirements provided back to companies to answer.[29] This augmentation of intelligence personnel at the battalion and company level coupled with thorough communications, enables intelligence officers to focus on and answer critical questions facilitating operations that positively influence the local population and subvert enemy influence.

In addition to augmenting lower-level intelligence organizations, MG Flynn cites other best practices from regimental and brigade intelligence units such as proactive advertisement of collection and production capability and the production of written intelligence summaries that incorporate everyone's activities in the area of operations.[30] Additionally, the report recommends the creation of what the authors call, "Stability Operations Information Centers" where select intelligence analysts will produce written comprehensive assessments of pivotal regions based on all available information.[31] These analysts, unlike those in current intelligence fusion centers, will operate at lower classification levels and establish areas where local citizens and leaders as well as representatives from NGOs and other organizations can share and exchange information over cups of tea.[32] The information centers will serve as single nodes for obtaining critical environmental information that can be used to positively influence the population and world opinion while disrupting the enemy's ability to effectively use intimidation and terror as a weapon.

The author's own experiences in Al Anbar Province, Iraq in the fall of 2005 provide additional evidence of the need for Stability Operations Information Centers where

comprehensive population-centric information can be quickly obtained and utilized by tactical units. As the intelligence officer for the 13th Marine Expeditionary Unit (MEU), the author coordinated closely with the Marine Corps Tactical Fusion Center (TFC) to gather information with only a few days notice prior to commencing operations. Coming directly from Exercise Bright Star in Egypt, the MEU was not assigned an area of operations until just days before conducting operations. Initially, the MEU was tasked with conducting COIN operations in Ar Rutbah and securing the main lines of communication (LOCs) from the Jordanian border through Rutbah to west of Ramadi. After several weeks, the MEU was ordered to clear and then conduct COIN operations in Hit. The information provided by the TFC was almost exclusively focused on insurgent activity and composed primarily of unit significant activity (SIGACT) reporting. Since the information from the TFC was generally obtained through unit reporting, it may not be surprising that when the author conducted intelligence exchanges directly with the battalion intelligence officers in the areas, their information was considerably more detailed, accurate and current. Additionally, the battalion intelligence officers could provide some non-population centric information, but since the vast majority of their time was spent on the enemy, information of this type was simply lacking. The establishment of an element dedicated to non-population centric information able to coordinate and visit directly with units on the ground will significantly assist in improving intelligence support to IO.

As discussed, many of the findings and recommendations from MG Flynn's report can be directly applied to improve MAGTF intelligence support to the "Four Block War." In such expeditionary conflicts, MAGTF intelligence personnel will be required to quickly develop and maintain a detailed picture of the enemy, environment and population in order to defeat the enemy and positively influence the local population as well as regional and world opinion. The

need to focus on both the enemy and the population cannot be overstated and will require intelligence personnel supporting IO from higher headquarters to be pushed down to the battalion and company levels in order to augment their efforts and fully understand and determine how IO can best be used at the local levels and above. The creation of an information center with the incorporation of MAGTF intelligence analysts, foreign disclosure officers, interagency personnel and areas where they, local citizens and leaders as well as NGO personnel can exchange information will be critical to providing relevant intelligence support to IO and achieving information superiority. Additionally, intelligence support to IO in a "Four Block War" will require MAGTF intelligence personnel to draw significantly upon previously collected information concerning the area of interest and reach back to experts in the U.S. and around the world. The idea of reach back support is certainly not new to intelligence personnel, but the ability for Marines to draw on centralized support for IO has recently been enabled by the creation of the Marine Corps Information Operations Center (MCIOC) at Quantico, Virginia.

THE MARINE CORPS INFORMATION OPERATIONS CENTER

The development of the MCIOC is part of the recent 202K Congressional plus up of the Marine Corps and is partially in response to the many challenges Marines continue to face regarding the development and implementation of effective IO in Iraq and Afghanistan as well as the recognition of the increasing importance of IO. According to Marine Corps Order 3120.10, Marine Corps Information Operations Program, released on 30 June 2008:

> "The MCIOC will provide MAGTF commanders and the Marine Corps a responsive and effective full-spectrum IO planning and psychological operations (PSYOP) delivery capability by means of deployable support teams and a comprehensive general support IO reach-back capability in order to support the integration of IO into Marine Corps operations. This includes, but is not limited to IO subject matter experts (SME) in: (1) Mission planning, (2) Threat and nodal analysis, (3) Electronic Warfare, (4) Military Deception, (5) Operations Security, (6) Psychological Operations, (7) Computer Network Operations, (8) The supporting capability of

Combat Camera, (9) The related capability of civil military operations, (10) Regional IO target expertise."[33]

The MCIOC will accomplish these missions assisted by the dedicated support of Marine Corps intelligence personnel and civilian analysts permanently assigned to the new command and fully deployable to support the MAGTFs and Joint Task Force (JTF) Commanders. The creation of the MCIOC will enable intelligence personnel at the MAGTFs to coordinate closely with IO experts able to leverage service and national resources to assist in rapidly building an understanding of the information environment and developing the tools and products required to gain and maintain information superiority.

The intelligence section of the MCIOC, or the "Threat Analysis Division," is comprised of approximately thirty-four permanently assigned personnel to include roughly twenty government employees and contractors, six Marine Officers and eight Enlisted Marines.[34] The division is responsible for the following seven key tasks:

1. Act as the repository of corporate knowledge and situational awareness necessary to facilitate the discovery and retention of IO specific skills, knowledge, and tools. This repository will augment Marine Corps IO support teams for service with the MAGTFs.
2. Provide fused IO threat event reporting, IO intelligence products, IO targeting support and other support as required, through close coordination with DIRINT, MCNOSC, DoD and OGAs.
3. Analyze adversary capabilities, vulnerabilities, networks, measures of effectiveness, and IO target information in order to develop applications that expedite the attribution of an attack and the delivery of integrated intelligence support to IO support teams.
4. Synchronize and coordinate with the Marine Corps Intelligence Activity (MCIA) to provide threat information regarding the technical capabilities and behavioral, psychological, and cultural aspects of individuals, organizations, and societies of IO interest.
5. Employ technical capabilities for improving collection, analysis and dissemination.
6. Provide target fidelity to prepare effective IO strategies and plans.
7. Leverage existing joint and inter-agency capabilities for IO nodal and infrastructure analysis resident in organizations such as the Joint Warfare Analysis Center.[35]

When fully operational, the "Threat Analysis Division" is expected to include four main sections: Influence Operations, Network Warfare Operations, Target Information, and

Intelligence Support. The Influence Operations section will assess target audience accessibility in the information environment and identify cultural influences to support determining means and lines of persuasion. The Network Warfare Operations section will support computer network operations through network nodal analysis. The Target Information section will create, augment, and/or leverage lethal and non-lethal targeting packages on Target Audiences (TA), High Value Targets (HVTs), and High Value Individual (HVIs) in the Operational Environment. Finally, the Intelligence Support to IO section will provide support to PSYOP, EW, MILDEC, OPSEC, CNO, PA, and CMO.[36] Importantly, the MCIOC will also establish a Regional Reach-back Element (RRE) as part of a Regional Reach-back Support Center (RRSC) dedicated to providing round-the-clock IO support to the Marine Corps, Joint Forces and Coalition Partners. As the name indicates, this twenty-two person element will be organized by region to include four teams focused respectively on the Middle East, Pacific, Europe and Africa, and South and Central America. Each element will be composed of an IO planner, PYSOP planner, political/military analyst, media analyst, and a threat analyst to provide a full range of support.[37]

The MCIOC is also incorporating important lessons learned from the 1st IO Command (Land) Iraqi Reach Back Team from operations conducted from 2004 to 2009. Importantly, individuals previously assigned to this organization are now located at the MCIOC and provide indispensable guidance and contributions to the development of intelligence tactics, techniques, and procedures (TTPs) regarding IO. In particular, the group determined six significant areas requiring attention and improvement. First, the commander's end state was either not considered or not highlighted during IO analysis and planning. Secondly, the target audience was either not identified or identified in such a general way that it was not useful. Additionally, although the operational environment was well understood, the information environment was not understood.

Also, intelligence personnel provided limited support to IO and generally had a weak understanding of IO. The IO planners did not properly or consistently engage with intelligence personnel. Lastly, the relationship between intelligence analysts and IO planners needs to be developed in order to ensure full coordination throughout the planning process and particularly during the development of intelligence support products. Based on these lessons learned, the MCIOC developed a process in which the intelligence analysts work closely with the IO planners to enable the development of an effective IO concept of support.

The intelligence support process outlined by the MCIOC coincides with current IO doctrine and emphasizes close collaboration between the IO planners and intelligence analysts in order to ensure IO planners and commanders receive the requisite support. The process begins with understanding the Commander's end state and proceeds to the identification of an individual or individuals who can impact that desired end state. The intelligence personnel then conduct collection and analysis to gain an understanding of the individuals and their information environment. The next step is to determine how those individuals leverage information in the information environment and provide the IO planners with intelligence products depicting trends, strengths, vulnerabilities, considerations, and intelligence gaps. This process is continuous and aimed at providing the IO planner with the information needed on the target audience and their information environment.

IO TRAINING AND SUPPORT FOR MAGTF INTELLIGENCE PERSONNEL

Although the previously described process should work well for intelligence personnel familiar with IO and with access to the required information, there may be challenges for those without IO training or the necessary data. The MCIOC is currently taking the lead in addressing the specific training requirements for intelligence personnel who will support IO with the Marine

Corps Training and Education Command (TECOM). Although the specific details of the training are being developed, immediately including basic IO instruction in the curricula of all levels of intelligence training would improve the understanding and support of IO in the MAGTF.

Currently, the all-source intelligence analyst (MOS 0231) basic course does not include any specific IO training.[38] The curriculum for the 0231 basic course is based on the requirements presented in the Intelligence Training and Readiness (T&R) Manual. The T&R manual does not explicitly include the requirement for all-source intelligence analysts to specifically provide support to IO.[39] In fact, the Intelligence T&R Manual only specifically includes IO related intelligence training for the 0202 MAGTF Intelligence Officer with the training requirement is listed only as, "Describe the factors to consider when planning intelligence support to Information Operations (IO)."[40] The instructors at the Navy and Marine Corps Intelligence Training Center (NMITC) recognize the importance of IO and include 1.5 hours of informal lecture and practical application concerning IO in the MAGTF Intelligence Specialist Career Course. This includes training and application of IO specific IPB as well as IO principles. Additionally, three hours of CLIC training is conducted during the career course that includes some intelligence support to IO.[41] This training is included by the instructors as "lesson purpose" or informal training and is limited in duration because of the lack of a specified requirement in the T&R manual or demand from the Fleet Marine Force.[42] The lack of emphasis on intelligence training to support IO is inconsistent with the aforementioned MCO 3120.10 that states,

"Fundamental changes in the global strategic environment have created conditions in which Information Operations (IO) will serve a critical role in achieving our military strategy and national security objectives.…The Marine Corps Information Operations Program (MCIOP) seeks to integrate information operations down to the lowest levels of the Marine Corps in order

to deny or degrade the ability of hostile and non-hostile actors to disseminate their message and, if desired, to modify it to our benefit while simultaneously preventing those same hostile messages from negatively affecting our own decision making processes. Integration of IO will be an essential part of our routine operations in the expeditionary and joint environments. Properly executed, it can help prevent a crisis or conflict; failing prevention, IO can both mitigate adversaries' actions and enhance our own."[43]

Based on the widely recognized importance of IO, the Intelligence T&R Manual should be revised to include specific training requirements for all intelligence personnel at all levels. In addition to training on specific techniques for IO related IPB, analysts need to understand the important differences between PA and PSYOPS and MILDEC. As discussed, the battles for Fallujah demonstrate the importance of a proactive, intelligence-supported PA effort. However, it is important for intelligence personnel to understand that PA efforts must be absolutely legitimate to ensure credibility while PSYOPS and MILDEC are separate disciplines that can utilize other methods to influence the enemy and target populations. While the T&R manual is under revision, basic intelligence support to IO techniques and procedures developed by the MCIOC should be immediately incorporated in NMITC courses.

Although the development and implementation of IO training for all Marine intelligence personnel will improve intelligence support to IO in the MAGTF, without the base line information and intelligence required for expeditionary operations, MAGTF intelligence will likely fall short. The expeditionary nature of MAGTF operations will require the rapid acquisition and development of intelligence. This requirement for rapid intelligence support to operations is not new and drives MAGTF intelligence personnel to ensure they have access to base line intelligence products such as the Joint Expeditionary Support Product (JESP). The JESP is a classified intelligence product developed by the collaborative efforts of the Department of State, several national intelligence agencies and service intelligence centers. The JESP provides critical historical, physical and political information concerning various nations and is

essential during initial planning since it provides the locations and details of key facilities such as embassy buildings, airfields, landing zones, port facilities, hospitals and government buildings. In order to insure MAGTF intelligence analysts have the appropriate information and intelligence to support IO, the development of an IO JESP would significantly enhance expeditionary intelligence support to IO. The IO JESP should also be developed through the collaborative efforts of the Department of State, national intelligence agencies, service intelligence centers, and of course the MCIOC. This product should be constructed for all areas Combatant Commanders and HQMC designate as a priority with a likelihood of MAGTF employment. The IO JESP should, at a minimum, provide intelligence personnel with such key IO details as media and communications nodes, cultural information, national, regional and local leadership information, Open Source Intelligence (OSINT) sites of interest and basic IO IPB products. The incorporation of these products into the JESP production process would promote regular updates and ensure accuracy, timeliness and relevancy of information.

In addition to the aforementioned IO training and products, it is imperative for intelligence analysts to also understand the areas of EW and CNO. Although an in-depth discussion of these areas is beyond the scope and classification of this paper, recent examples demonstrate the increasing importance of CNO and EW. In particular, Hezbollah's use of CNO, EW and MILDEC during their conflict with Israel in August 2006 provides excellent examples germane to future operations. Hezbollah's performance prior to and during the conflict with Israel in 2006 provides useful insights on how potential adversaries may use EW and CNO in the future. Before the conflict began, Hezbollah maintained tight security around their organization and planned operations while acquiring technology and training to enable successful EW and CNO.[44] During the conflict, Hezbollah employed basic cell phone intercept techniques to listen

to the conversations between Israeli soldiers and then use the information to promulgate the perception that they were able to intercept encrypted Israeli radio traffic.[45] The belief that Hezbollah could effectively intercept and decrypt Israeli radio communications caused significant concern for the Israelis as well as their allies who employed similar technology. Additionally, Hezbollah effectively used television, radio and internet resources to communicate their message and view of the conflict. Since Hezbollah maintains its own television broadcast, Al-Manar, they could transmit dedicated and focused coverage of events based on their perceptions and goals. These transmissions, although clearly biased, were picked up by several television and internet media outlets to include Al Jazeera, Al Arabiya, CNN and BBC, and contributed to a perception of Israeli aggression and heavy handedness.[46] These factors also aided Hezbollah in achieving their stated goal of humiliating Israel by sheer survival.[47]

Additionally, a photographer working for Reuters digitally manipulated a photo to make Israeli bombing appear worse than in actuality.[48] Although the photographer's links to Hezbollah are disputed, his failed attempt to influence opinion against Israel provides an important lesson on collaboration and reach-back. After Reuters published the photograph, an independent website and associated bloggers recognized possible manipulation and questioned the authenticity of the image.[49] Along similar lines, it is important to note that when Al-Manar was confronted with Israeli hacking attempts to shut down their satellite broadcasts, they used hacking and internet hijacking techniques to get their message out. Hezbollah hackers searched for vulnerable sites where they could hijack an existing IP address and establish their own site.[50] Although this was an effective means for Hezbollah, one particular attempt was detected and thwarted by an independent group of internet researchers who track jihadist activity on the internet.[51] These examples demonstrate the importance of understanding an adversary's

capabilities and how encouraging a collaborative community approach can assist in countering an enemy's IO effort.

CONCLUSION AND RECOMMENDATIONS

The Marine Corps' recognition of the importance of IO in current and future conflict is illustrated in the "Four Block War" concept and demonstrated through the creation of the MCIOC. The ability of MAGTF intelligence professionals to provide the required intelligence support to IO can be enhanced through improvements to doctrine, an IO emphasis in training, the establishment of specific IO population-centric intelligence cells at the tactical level, the development and maintenance of IO specific base line intelligence products, and the development of collaborative communities to counter enemy IO efforts. Specifically, the following recommendations provide actions the Marine Corps can take to improve overall MAGTF intelligence support to IO.

- Develop tactics, techniques and procedures for intelligence analysts conducting IPB in support of IO.
- Encourage MAGTF intelligence personnel to have a proactive IO focus and ensure they have the tools and training to support IO and PA efforts.
- Ensure IO billets are filled to 100 percent at all MAGTF levels.
- Incorporate recent IO case studies in intelligence training.
- Ensure IO trained intelligence analysts are pushed down to the battalion and company levels.
- Create "information centers" separated from intelligence centers where population centric information can be gathered and exchanged.
- Ensure all MAGTF intelligence personnel understand the roles and capabilities of the MCIOC and how to leverage those capabilities.
- Include specific IO training requirements in the Intelligence T&R manual for all MAGTF intelligence personnel.
- Incorporate tailored IO training in to all MAGTF intelligence instruction at NMITC.
- Establish the requirement for and provide support to the development of an IO JESP.
- Spearhead the development of virtual IO collaborative communities to assist in monitoring and countering adversary IO.

As the Marine Corps prepares for the hybrid wars of the future, it is clear that information operations will play a critical role in the success of the MAGTF. Based on lessons learned

from previous and ongoing conflicts, these eleven actions would significantly enhance intelligence support to IO, enabling intelligence to drive operations and contributing significantly to MAGTF success in expeditionary operations.

Notes

[1] The National Intelligence Council, *Global Trends 2025: A Transformed World* (Washington, DC: U.S. Government Printing Office, November 2008), 1.

[2] Charles C. Krulak, "The Strategic Corporal: Leadership in the Three Block War," *Marine Corps Gazette*, Jan 1999: 20.

[3] Lieutenant General James N. Mattis and Lieutenant Colonel Frank G. Hoffman, "Future Warfare: The Rise of Hybrid Wars," *Proceedings*, November 2005: 19.

[4] The National Intelligence Council, p. 1.

[5] The National Intelligence Council, p. 23.

[6] The National Intelligence Council, p. 51.

[7] Marine Corps Warfighting Publication 3-40.4, Marine Air-Ground Task Force Information Operations, pp. 1-2.

[8] Marine Corps Warfighting Publication 3-40.4, pp. 1-6.

[9] Marine Corps Warfighting Publication 3-40.4, pp. 1-3.

[10] Marine Corps Warfighting Publication 3-40.4, pp. 2-3.

[11] Based on personal experience and conversations with MCIOC personnel.

[12] Joint Publication 2-01.3, Joint Intelligence Preparation of the Operational Environment, p. II-33.

[13] G.J. David Jr. and T.R. McKeldin III, *Ideas as Weapons: Influence and Perception in Modern Warfare* (Dulles, VA: Potomac Books, 2009), 332.

[14] David Jr. and McKeldin III, p. 348.

[15] David Jr. and McKeldin III, p. 342.

[16] David Jr. and McKeldin III, p. 342.

[17] David Jr. and McKeldin III p. 348.

[18] Lieutenant General Thomas F. Metz, "Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations," *Military Review*, May-June 2006: 109.

[19] Metz, p. 109.

[20] Metz, p. 110.

[21] Metz, pp. 110-112.

[22] Major General Michael T. Flynn, Captain Matt Pottinger, and Paul D. Batchelor, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Center for a New American Security, Washington DC, January 2010, p. 4.

[23] Flynn, Pottinger, and Batchelor, p.7.

[24] Flynn, Pottinger, and Batchelor, p.7.

[25] Flynn, Pottinger, and Batchelor, p.8.

[26] Flynn, Pottinger, and Batchelor, p.8.

[27] Flynn, Pottinger, and Batchelor, p.9.

[28] Flynn, Pottinger, and Batchelor, p.13.

[29] Flynn, Pottinger, and Batchelor, pp.13-14.

[30] Flynn, Pottinger, and Batchelor, p.16.

[31] Flynn, Pottinger, and Batchelor, p.19.

[32]Flynn, Pottinger, and Batchelor, p.19.

[33] Marine Corps Order 3120.10 Marine Corps Information Operations Program, 30 June 2008, p. 2.

[34] Marine Corps Information Operations Center, Threat Analysis Division Power Point Brief dated 27 October 2009.

[35] Marine Corps Information Operations Center

[36] Marine Corps Information Operations Center

[37] Marine Corps Information Operations Center

[38] E-mail exchange with Gunnery Sergeant Joseph L. Davila, Director of the MAGTF Intelligence Specialist Entry Course, Dam Neck, Virginia, 15 December 2009.

[39] United States Marine Corps, Intelligence Training and Readiness Manual, 20 August 2004. Accessed at http://www.marines.mil/news/publications/Documents/MCO%203500.32%20W%20ERRATUM.pdf on 16 January 2010.

[40] United States Marine Corps, Intelligence Training and Readiness Manual, 20 August 2004, p.41.

[41] E-mail exchange with Gunnery Sergeant Raymond A. Boyce, Director of the MAGTF Intelligence Specialist Career Course, Dam Neck, Virginia on 16 December 2009.

[42] E-mail exchange with Gunnery Sergeant Boyce on 16 December 2009.

[43] Marine Corps Order 3120.10 Marine Corps Information Operations Program, 30 June 2008, p. 1.

[44] David A. Acosta, "Hizballah: Deception in the 2006 Summer War," *IOSPHERE*, Winter 2008: 18.

[45] Acosta, p. 19.

[46] Acosta, p. 21.

[47] Acosta, p. 16.

[48] Acosta, p. 21.

[49] Acosta, p. 21.

[50] Acosta, p. 22.

[51] Acosta, p. 22.

Bibliography:

Acosta, David, A. “Hizballah: Deception in the 2006 Summer War.” *IOSphere*, Winter 2008: 15-23.

Anderson, Donald, J. *Cultural Intelligence: Meeting Today’s Demands*. Newport, RI: Naval War College, Joint Military Operations Department, May 2004. http://www.au.af.mil/au/awc/awcgate/navy/nwc_anderson.pdf

Applegate, Melissa A. *Preparing for asymmetry: As seen through the lens of Joint Vision 2020 (Studies in asymmetry).* Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2001. http://www.au.af.mil/au/awc/awcgate/ssi/preparng.pdf

Bartles, Charles, and Lester Grau. “FMSO-JRIC - The War Ahead and the Way Ahead.” *FMSO,* http://fmso.leavenworth.army.mil/documents/war-ahead.htm

Best, Richard A. *Intelligence Issues for Congress.* CRS Report for Congress RL 33539. Washington, DC: Congressional Research Service, December 18, 2007. http://www.usembassy.it/pdf/other/RL33539.pdf

Boot, Max. “What the Past Teaches about the Future.” *Joint Forces Quarterly*. Issue 44, 1st Quarter 2007. http://www.ndu.edu/inss/Press/jfq_pages/editions/i44/JFQ44%20boot.pdf

Boot, Max. “The Struggle to Transform the Military.” *Foreign Affairs*, Mar/Apr 2005, Vol. 84, Issue 2: 109-116. http://www.cfr.org/publication/8028/struggle_to_transform_the_military.html

Bowden, Mark. *Killing Pablo: The Hunt for the World's Greatest Outlaw.* New York: Atlantic Monthly Press, 2001.

Brimley, Shawn, and Vikram Singh. “Averting the System Reboot: Innovations and Critical Lessons from Iraq Must Be Preserved.” *Armed Forces Journal*, December 2007. http://www.armedforcesjournal.com/2007/12/2981245

Callwell, C. Eoo. *Small Wars: Their Principles and Practice (Third Edition, 1901).* Lincoln and London: University of Nebraska Press, 1996.

Chairman of the Joint Chiefs of Staff. *National Military Strategy of the Unites States of America A Strategy for Today; A Vision for Tomorrow. 2004.*

http://www.defenselink.mil/news/mar2005/d20050318nms.pdf

Clark, Major Todd J. “Developing a Cultural Intelligence Capability.” U.S. Army Command and General Staff College, December 2008.
http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA502169&Location=U2&doc=GetTRDoc.pdf

Clark, Wesley K. ‘The Next War.” *Washington Post*, September 16, 2007
http://www.washingtonpost.com/wp-dyn/content/article/2007/09/14/AR2007091401973.html

Collins, Matthew. “Beyond the Van Riper Plan.” *Marine Corps Gazette*, Oct 2006, 24-26.

Commandant of the Marine Corps, Commandant of the Coast Guard, and Chief of Naval Operations. *A Cooperative Strategy for 21st Century Sea Power*. November 2007
http://www.navy.mil/maritime/MaritimeStrategy.pdf

Commandant of the Marine Corps and Chief of Naval Operations. *Naval Operating Concept 2006*, September 1, 2006.
https://www.mccdc.usmc.mil/CIW/ER/Naval%20Operations%20Concept.pdf

Commandant of the Marine Corps. *Marine Corps Strategy* 21. November 3, 2000.
Concepts and Plans Division, MCWL. “Irregular Warfare: New concepts for consideration.” *Marine Corps Gazette*, Oct 2007, 26-27.

Dailey, Dell. “An 'All Elements of Power' Strategy for Combating Terrorism.” *The Washington Institute for Near East Policy*, December 18, 2007. http://www.washingtoninstitute.org

David, G.J, Jr. and T.R. McKeldin, III. *Ideas as Weapons: Influence and Perception in Modern Warfare*. Dulles, VA: Potomac Books, 2009.

Dinsmore, Captain Jeffrey. “Intelligence Support to Counterinsurgency Operations.” *Marine Corps Gazette*, Ju1 2007, 13-16.

Downes, Eric S. “Intelligence Reachback.” *Marine Corps Gazette*, Dec 2005, 21-23.

Ennis, Colonel Michael. “The Future of Intelligence.” *Marine Corps Gazette*, Oct 1999, 46-48.

Felter, Joseph, and Brian Fishman. Al Qa'ida's Foreign Fighters in Iraq: A First Look at the Sinjar Records. West Point, NY. December 20, 2007.
http://www.ctc.usma.edu/harmony/pdf/CTCForeignFighter.19.Dec07.pdf

Flynn, Major General Michael T., Captain Matt Pottinger, and Paul D. Batchelor. “Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan.” Washington, DC: Center for a New American Security, January 2010.

Gan'ett, Keith. “Restructure of Remotely Sensed Imagery Intelligence.” *Marine Corps Gazette*,

Apr 2006, 36-40.

Glieco, Patlick A. “Achieving Persistent Surveillance Requires Community Effort to Build One Continuum.” *Pathfinder,* November/ December 2007, 19-22.

Grau, Lester. “Guerrillas, Terrorists, and Intelligence Analysis: Something Old, Something New.” *Military Review*, July 1, 2004.
http://usacac.army.mil/CAC/milreview/download/English/JulAug04/grau.pdf

Harding, Steve. “Training Arabic Linguists.” *Soldiers Magazine.* May 2004.
http://usarmy.vo.llnwd.net/e1/soldiers/archives/pdfs/may04all.pdf

Headquarters U.S. Marine Corps. Marine *Corps 2005-2015 Draft ISR RoadMap. Version 1.1.* Washington, DC: Headquarters U.S. Marine Corps, October 2, 2006.
https://192.156.75.123/OpsDiv/Integration/Intel/intelligence_integration_files/Roadmap%20Draft--4%20oct.doc

Headquarters U.S. Marine Corps. *Marine Corps Concepts for a Changing Security Environment.* Washington DC: Headquarters U.S. Marine Corps, June 2009.

Headquarters U.S. Marine Corps, Intelligence Department. *OSD Language Initiatives: Defense Language Transformation Roadmap. 2009.*

Headquarters U.S. Marine Corps. *United States Marine Corps Concepts and Programs.* Washington, DC: Headquarters U.S. Marine Corps, 2009.

Higgins, LtCol James B. “Culture Shock: Overhauling the Mentality of the Military.” *Marine Corps Gazette,* Feb 2006, 48-51.

Hoffman, LtCol (Ret) F.G. “Preparing for Hybrid Wars.” *Marine Corps Gazette,* Mar 2007, 57-61.

Hoffman, LtCol (Ret) F.G. “The Corps' Expansion, Strategic Risks and Benefits.” *Marine Corps Gazette,* Jun 2007, 42-44.

Johnson, Kimberly. “Corps Creates Intel Cells at Rifle-Company Level.” *Marine Corps Times*, January 18, 2008.
http://www.marinecorpstimes.com/news/2008/01/marine_company_intel_080117/

Kinniburgh, James and Dorothy Denning. “Blogs and Military Information Strategy.” Joint Special Operations University, Hurlburt Field, Florida, 2006.

Krulak, Charles C. “The Strategic Corporal: Leadership in the Three Block War.” *Marine Corps Gazette.* Jan 1999.

Lively, Capt James W. “Cultural Education.” *Marine Corps Gazette,* Apr 2007, 21-25.

Livingston, SSgt Amos. “The Next Step for Intelligence.” *Marine Corps Gazette,* Feb 2007, 15-16.

Mann, Maj Morgan G. “Census Operations and Information Management.” *Marine Corps Gazette,* Apr 2006, 24-28.

Manwaring, Max G. “Street Gangs: The New Urban Insurgency.” *Strategic Studies Institute,* March 2005.
http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB597.pdf

Marine Corps Center for Lessons Learned. *Interagency Activity in Stability Operations.* May 18, 2007.

Marine Corps Center for Lessons Learned. *3rd Radio Battalion Post-Deployment Lessons and Observations Quick Look Report.* September 3, 2006.

Marine Corps Center for Lessons Learned. *Intelligence Enhancement in the Infantry Battalion: Producing Actionable Tactical Information.* May 21, 2007.

Marine Corps Center for Lessons Learned. *Intelligence Capability Enhancements: OIF Infantry Battalions Operation METRO.* January 4, 2007.

Marine Corps Center for Lessons Learned. *Intelligence Exploitation of Enemy Material.* June 20, 2006.

Marine Corps Center for Lessons Learned. *Intelligence and Surveillance Related Lessons from The Global War on Terrorism.* September 9, 2005.

Marine Corps Training and Education Command. *MOS 0211 Roadmap.*
http://www.tecom.usmc.mil/g3/MOSRoadmaps/0211-0291.pdf

Marine Corps Training and Education Command. *MOS 0231 Roadmap.*
http://www.tecom.usmc.mil/g3/MOSRoadmaps/0231-0291.pdf

Marine Corps Training and Education Command. *MOS 0241 Roadmap.*
http://www.tecom.usmc.mil/g3/MOSRoadmaps/0241-0291.pdf

Marine Corps Training and Education Command. *MOS 0261 Roadmap.*
http://www.tecom.usmc.millg3/MOSRoadmaps/0261-0291.pdf

Marine Corps Training and Education Command. *MOS* 2621 *Roadmap.*
http://www.tecom.usmc.mil/g3/MOSRoadmaps/2621-2691.pdf

Marine Corps Training and Education Command. *MOS* 2631 *Roadmap.* http://www.tecom.usmc.millg3/MOSRoadmaps/2631-2691.pdf

Marine Corps Training and Education Command. MOS 2671 Roadmap. http://www.tecom.usmc.mil/g3/MOSRoadmaps/2671-2691.pdf

Martin, Captain Zachary D. "By Other Means." *Marine Corps Gazette*, September 2005, 68-70. http://www.smallwars.quantico.usmc.mil/search/Articles/By%20Other%20Means.pdf

Mattis, Lieutenant General James N. and Lieutenant Frank G. Hoffman, USMCR(Ret.). "Future Warfare: The Rise of Hybrid Wars." *Proceedings*, November 2005, 18-19. http://milnewstbay.pbworks.com/f/future+warfare+hybrid+warriors.pdf

Metz, Lieutenant General Thomas F. "Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations." *Military Review*, May-June 2006.

Morgan, Rod. "Company Intelligence Support Teams." *Armor*, July-August 2008, 23-25. http://www.dami.army.pentagon.mil/offices/dami-zxg/documents/COIST-Armor%20Magazine-JUL-AUG08.pdf

Munson, Peter J. "Cultural Education and the Reading Program." *Marine Corps Gazette*, Jan 2006, 49-52.

National Intelligence Council, Project 2025, "Global Trends 2025: A Transformed World." November 2008. http://www.dni.gov/nic/NIC_2025_project.html

President of the United States. *National Security Strategy of the United States of America.* March 2006. http://www.strategicstudiesinstitute.army.mil/pdffiles/nss.pdf

Reiley, Matthew A. "Transforming USMC Intelligence to Address Irregular Warfare." *American Intelligence Journal*, Summer 2008, 50-59.

Russell, Charles A. and Robert E. Hildner. "Intelligence and Information Processing in Counterinsurgency." *Air University Review*, July-August 1973. http://www.airpower.au.af.mil/airchronicles/aureview/1973/jul-aug/russell.html

Shachtman, Noah. "U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets." *Wired*, October 19, 2009. http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/

Spencer, Emily and Tony Balasevicius. "Crucible of Success: Cultural Intelligence and the Modern Battlespace." *Canadian Military Journal*, March 2009. http://www.journal.dnd.ca/vo9/no3/07-spencer-eng.asp

United States Marine Corps. *Small Wars Manual.* New York: University Press of the Pacific, 2005.

U.S. Department of the Air Force. *Air Force Engagement in Expeditionary Warfare.* October 24, 2006. http://www.dtic.mil/ndia/2006expwarfare/henabray.pdf

U.S. Department of the Army. *Counterinsurgency.* FM 3-24. Washington, DC: U.S. Department of the Army, December 2006.

U.S. Department of Defense. *Defense Language Transformation Roadmap.* January, 2005. http://www.defenselink.mil/news/Mar2005/d20050330roadmap.pdf

U.S. Department of Defense. *National Defense Strategy of the United States of America.* June 2008. http://www.defenselink.mil/news/2008%20National%20Defense%20Strategy.pdf

U.S. Department of Defense. *Quadrennial Defense Review Report.* February 6, 2006. http://www.defenselink.mil/qdr/report/Report20060203.pdf

Appendix A

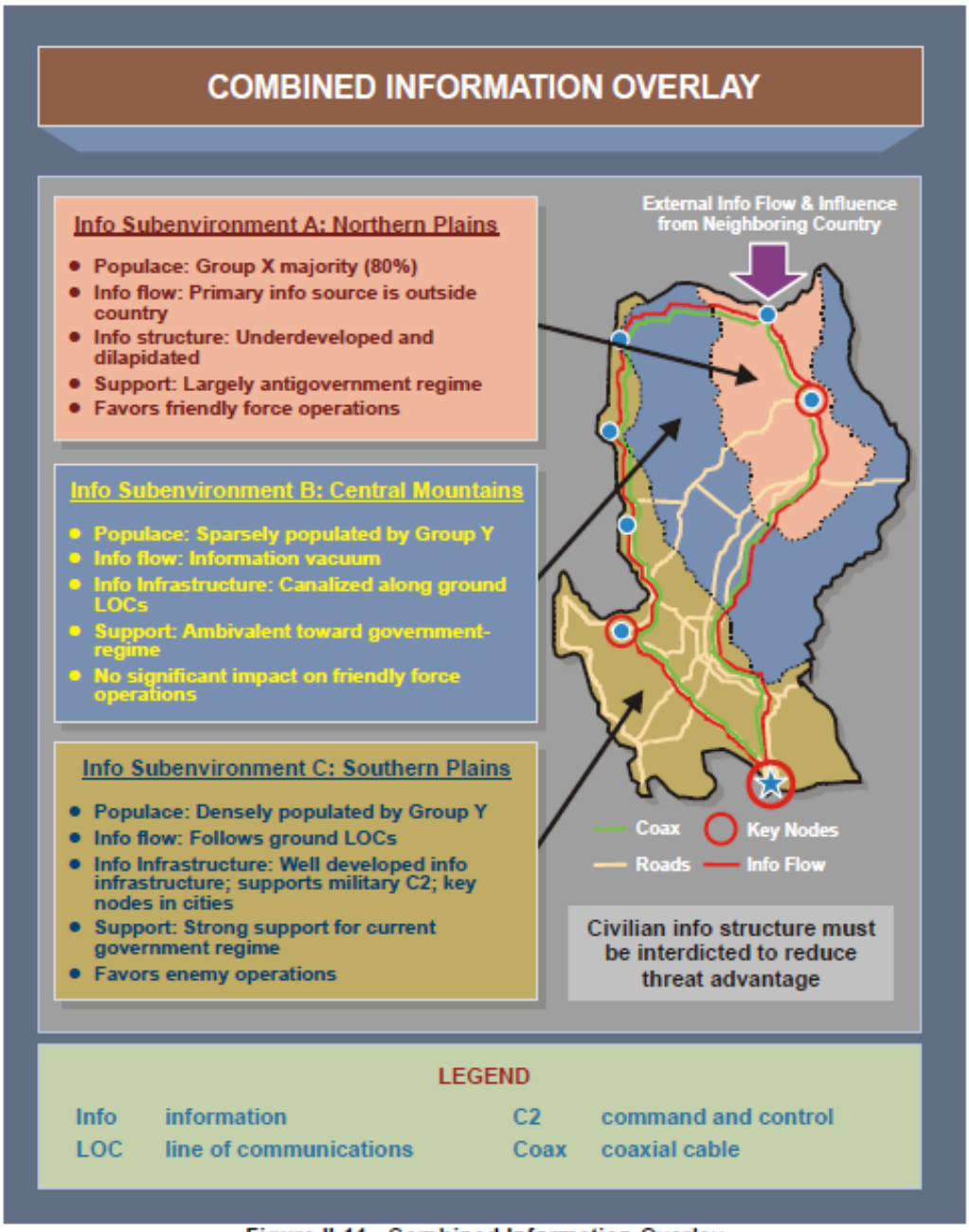

Figure II-11. Combined Information Overlay

Source: JP 2-01.3 Joint Intelligence Preparation of the Operational Environment, p. II-33.

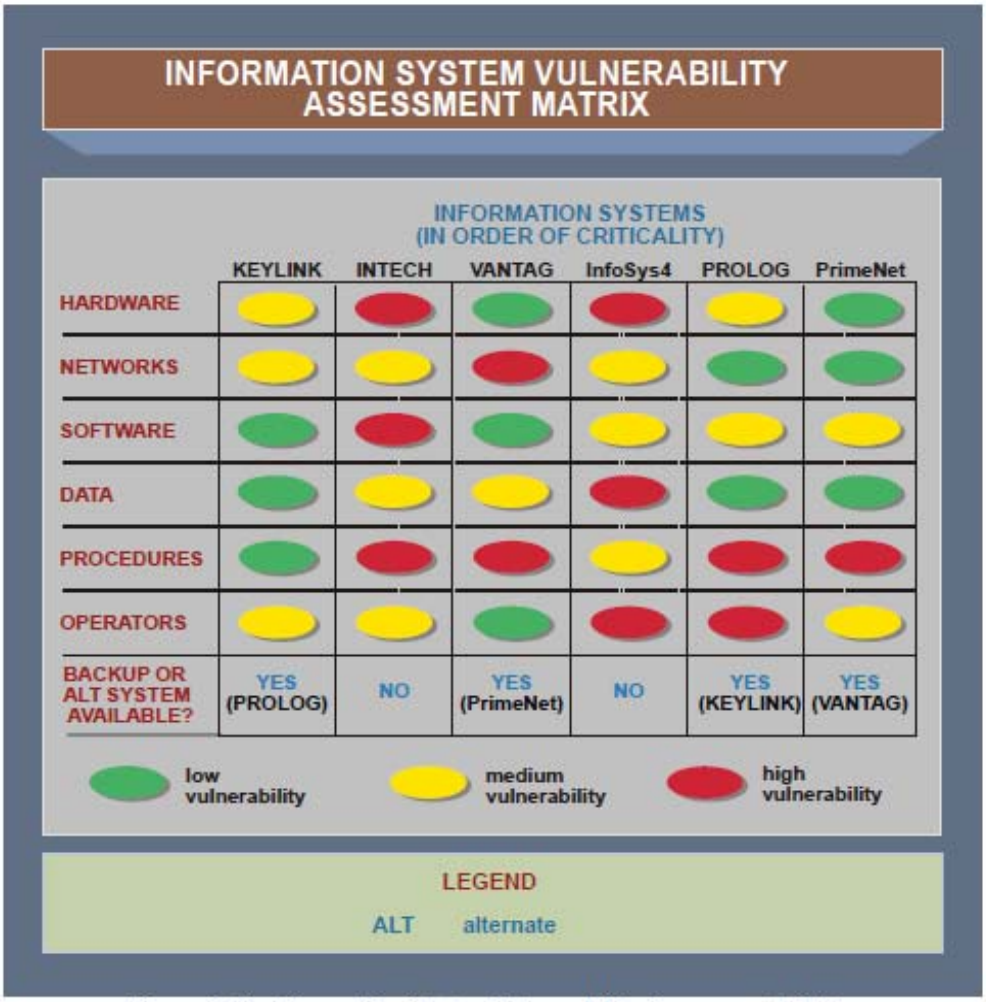

Figure II-12. Information System Vulnerability Assessment Matrix

Source: JP 2-01.3 Joint Intelligence Preparation of the Operational Environment, p. II-34.